**Android App反编译**

1. **背景**

以前了解过Android APP 的反编译技术，但是从来没有实战过，今天看到老师在课堂上展示反编译所以今天就实战一下，学习一下。

1. **技术介绍**

Android项目的JAVA源码，资源文件，XML文件这些是反编译想要得到的。所以就要用以下几个工具来从Android apk中获取。

**apktool**

作用：资源文件获取，可以提取出图片文件和布局文件进行使用查看

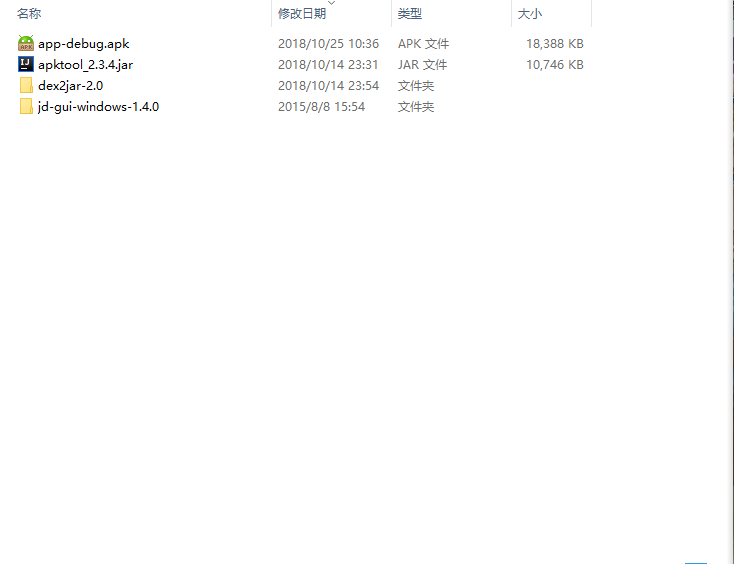
**dex2jar**

  作用：将apk反编译成java源码（classes.dex转化成jar文件）

**jd-gui**

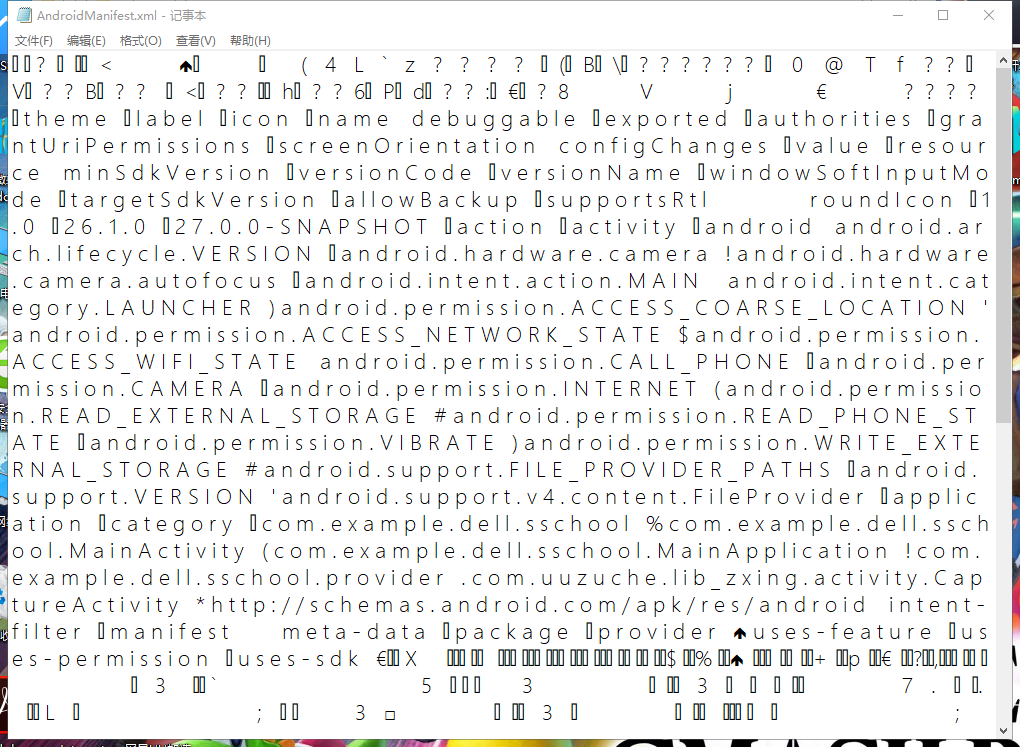
作用：查看APK中classes.dex转化成出的jar文件，即源码文件

1. 实战
2. **首先反编译一个我自己写的APP，没有经过反编译处理，看一看效果**
3. **准备工具：**



1. **用apktool获取xml资源文件：**
   1. APK直接解压打开也可以看到XML文件，但是XML已经加密看到乱码：

AndroidManifest.xml:



* 1. 所以要用apktool工具将将资源文件解密

打开cmd 到目录

执行apktool.jar

Java -jar apktool\_2.3.4.jar d -f app-debug.apk -o MMTS



打开目录可以看到反编译好的文件



这时打开xml资源文件就可以正常显示了：

AndroidManifest.xml:

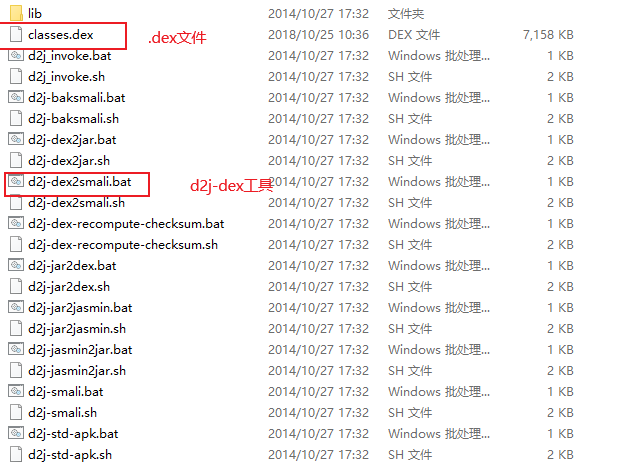


1. **使用dex2jar反编译apk得到Java源代码**

找到目录下的classes.dex文件。

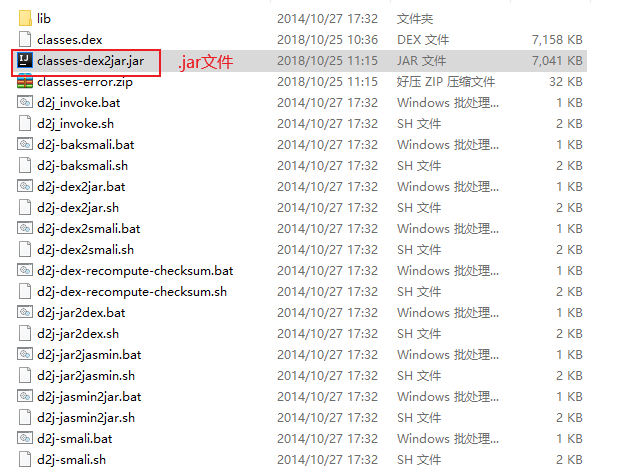


将它们放到dex2jar下的目录中。

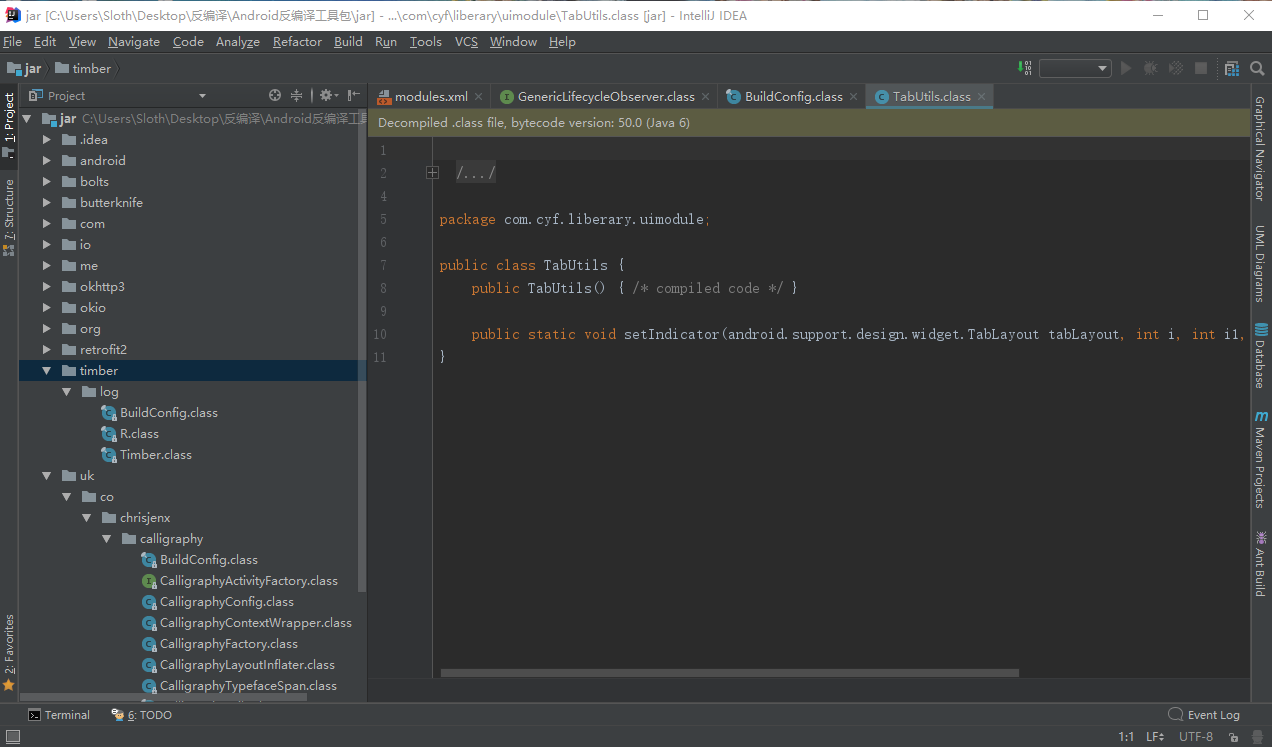


并调用 命令就能将.dex文件转化为.Jar文件jar文件就能通过jd-gui直接查看





1. **通过jd-gui进行查看**

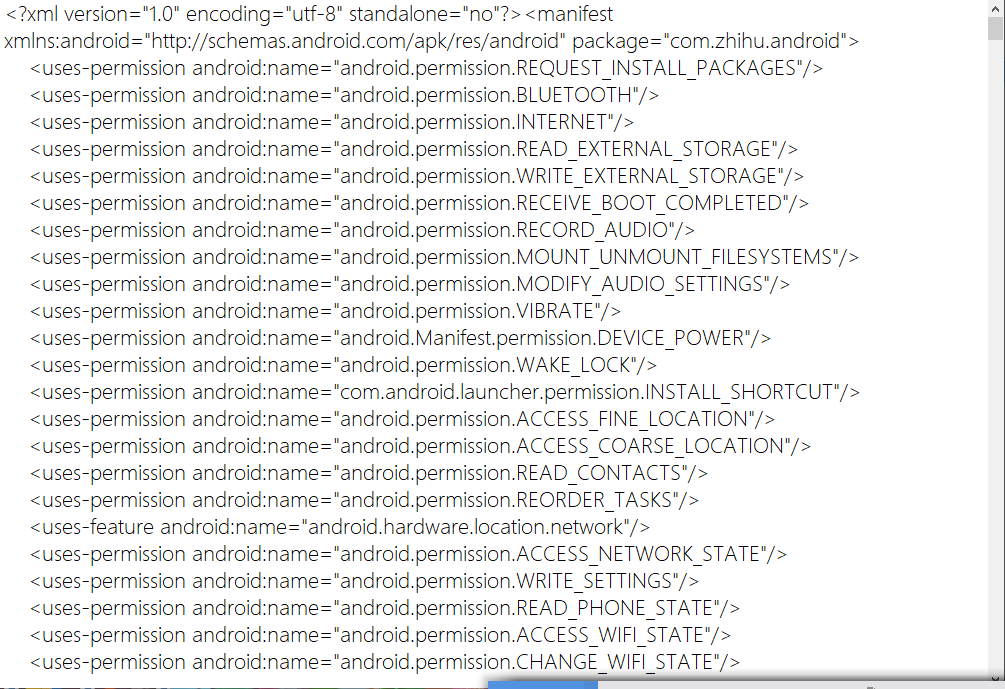
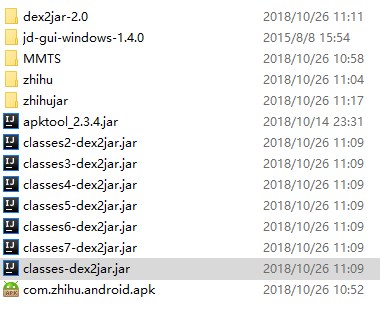


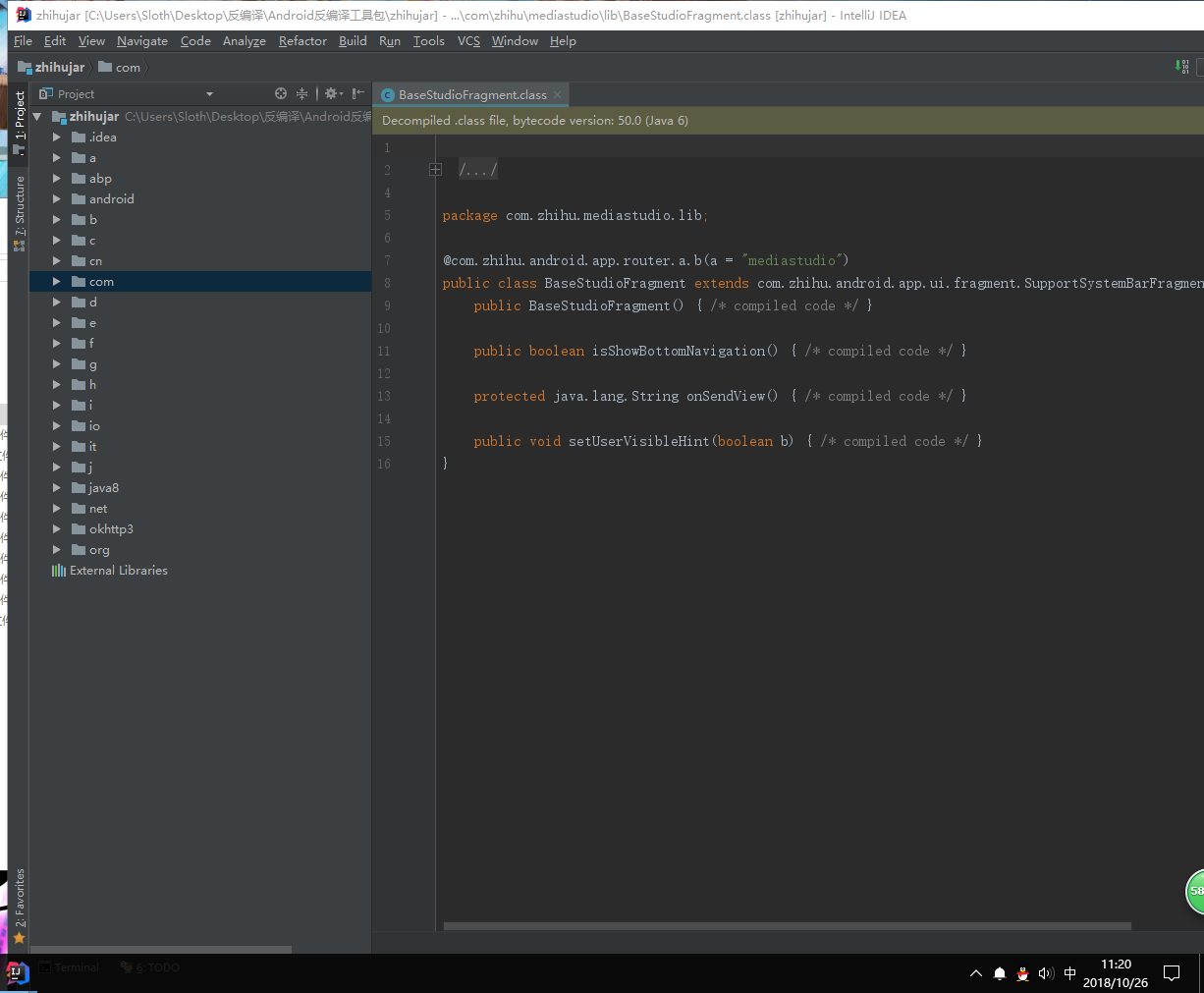
可以看到库文件，和所写的代码，因为我写的这个APP没有进行混淆处理所以变量名正常显示。

1. 反编译其他APP

我们可以通过相同的方式查看其他上线APP

以知乎为例：





可以看出知乎的已经做了混淆处理，很多的包名,方法名都变成了a,b,c,查看起来非常费时费力。不过也可以看出知乎集成了什么开源库，什么API 比如 OKhttp3 网络请求框架；alipay ;高德地图api等等还是很有参考价值的